## REMARKS/ARGUMENTS

***Status of the Claims***

Before this Amendment, claims 1, 2, 4-18, 20-27, 29-35, and 59 were examined. No claims are amended. No claims are presently added or canceled. Therefore, claims 1, 2, 4-18, 20-27, 29-35, and 59 remain present for examination, and claims 1, 17, 18, 21, 22, 25, and 29 are the independent claims.

The Office Action dated August 7, 2007 ("Office Action") rejected claims 1, 2, 4-17, 29-35, and 59 under 35 U.S.C. § 103(a) as being anticipated by U.S. Patent No. 6,101,477 to Hohle et al. ("Hohle") in view of U.S. Patent No. 5,414,772 to Naccache ("Naccache") and further in view of U.S. Patent No. 6,304,223 to Hilton ("Hilton"). The Office Action rejected claim 21 under 35 U.S.C. § 103(a) as being unpatentable over Hohle in view of U.S. Patent 6,226,744 to Murphy et al. ("Murphy") and further in view of Hilton and further in view of Naccache. The Office Action rejected claims 18, 20, 22, and 23-27 under 35 U.S.C. § 103(a) as being unpatentable over Murphy in view of Hilton and further in view of Naccache. Reconsideration is respectfully requested.

***35 U.S.C. §103(a) Rejections***

The Office Action rejected the independent claims under 35 U.S.C. § 103(a) as unpatentable over various combinations of Hohle, Naccache, Murphy, and Hilton. Factual findings made by the Office are the "necessary underpinnings to establish obviousness." MPEP § 2141(II). The Office must set forth "the relevant teachings of the prior art relied upon." MPEP § 706.02(j). Additionally, in *KSR* the Supreme Court noted that the analysis supporting a rejection under 25 U.S.C. § 103 must be made explicit. *See* MPEP § 2142. As will be discussed below, Applicants respectfully submit that the Office has erred as to the factual findings, and that the Office has not established a *prima facie* case of obviousness.

Certain independent claims generally set forth a secured data exchange between a smart card and a central computer system, via a smart card communication device. The exchange, wherein the smart card communication device receives the secure data and transmits the data through a *communication network* is not taught or suggested in the cited references.

More specifically, the references do not teach or suggest:

1) "transmitting the outgoing" signal "through a communication network" to a *remote* central computer system "without deciphering the data," as set forth in claim 1 or 23;

2) secured data formatted by the smart card to allow the central computer system to detect a modification to the secured data occurring during transmission beginning at the smart card, passing through a smart card communication device, and extending through to the remotely located central computer system, as generally recited in claims 1, 17, 21, 22 or 29; or

3) a second set of secured data, the second set formatted by the central computer system to allow the smart card to detect a modification to the second set occurring during transmission beginning at the remote central computer system, passing through a smart card communication device, and extending to the smart card, as recited in claim 17, 18, and 25. Thus, in selected embodiments, secure data is "not deciphered, decoded or authenticated anywhere within the communication link except at the smart card 106 and the smart card server 130" located in the central computer system 102 (Original Application, p. 10, ll. 7-9).

### **1. Secured Data Transmitted through a Network without Deciphering**

The Office has repeatedly conceded that "Hohle does not expressly disclose the outgoing transmission sent without deciphering the data" (Office Action, p. 3, ll. 18-19; Office Action dated December 29, 2006, p. 3, ll. 12-13; Office Action dated August 10, 2006, p. 4, ll. 9-10). Additionally, the Office Action has conceded that "Hohle does not teach ... using the smart card communication device to produce an outgoing secure data signal, and communicating to a central computer system that is remote from the smart card communication device" (Office Action, p. 3, ll. 19-22).

The Office Action appears to rely on Naccache to teach the missing elements. However, Applicants respectfully submit that the Office Action has erred in this reliance. Claim 1 recites a method for "establishing a secure communication link ... through a communication network." The smart card communication device "produce[s] an outgoing secure data signal . . .

without deciphering the secured data." The secure signal is transmitted over the communication network to a central computer system "remote from the smart card communication device."

Naccache, in contrast, describes a "chip card" and " a computer . . . comprising a chip reader enabling **physical communication** with the card," the interface shown as an "**I/O interface**" (emphasis added, Naccache, col. 3, ll. 33-45; Fig. 3). In fact, while in Naccache the communication is via the "interface," the Office Action relies on Naccache to teach communication between a smart card communication device and a remote central computer system (Office Action, p. 4, ll. 6-8, *citing* Naccache, col. 6, ll. 1-11).

This reliance is misplaced, as claim 1 recites communication over a "communication network." Communication over an "interface" clearly is different than communication over a "communication network" of claim 1.

Moreover, claim 1 recites a central computer system that is remote from the smart card. Naccache also fails to teach or suggest this element. Rather, the chip reader (Apparatus B) is a local computer in physical communication with a chip card. A *local* computer in *physical communication* fails to suggest the *remote* central computer system where transmission is through a *communication network.* Hence, the Office Action has erred in corresponding apparatus B with the (remote) central computer system (Office Action, p. 4, ll. 9).

Additionally, claim 1 recites a further step of "formatting the outgoing secure data signal in accordance with a communication network protocol." This additional step further illustrates differences between the claims and the local computer and interface set forth in Naccache.

### 2. & 3. Hohle fails to teach detecting a modification to the secured data occurring during transmission between the Smart Card and the Central Computer System

Various embodiments of the present invention set forth systems or methods for establishing a secure communication link *between* a *smart card* and a *central computer system,* wherein the secure data is *passed through a smart card communication device* remote from the central computer system. In some claims, central computer may detect a modification to the secured data beginning at smart card the and extending through to the central computer. In other embodiments, the detection relates to communication in the reverse direction. Again, it is worth noting that the central computer system is located remotely from the smart card and/or the smart card communication device.

Naccache does not appear to be cited for these limitations, as the Office Action appears to rely on Hohle to teach the missing elements (Office Action, p. 3, ll. 9-16; p. 8, l. 8; p. 9, l. 7, *citing* Hohle, col. 22, ll. 47-67). The Office Action indicates that it is the issuer 10 of Hohle that reads on the central computer system of the claims (Office Action, p. 3, l. 2, *citing* Hohle Fig. 10).

However, the cited passages of Hohle address "'signing' of the data using a message authentication code" for transmission between the card and an "external device" (Hohle, col. 22, ll. 50-57). Hohle does not suggest that the "external device" is the issuer 10. Instead, Hohle at one point describes the "external device" to be "a **card reader**" (Hohle, col. 3, ll. 3-4, emphasis added) and communication to the external device is through "a line for **serial** data communication" (Hohle, col. 3, ll. 24-25, emphasis added). A card reader and serial data communication fall far short of the end-to-end data integrity between a smart card and central computer system over a communication network in the claimed invention. Hence, Hohle also falls short of the claimed invention that describes end-to-end data integrity from a smart card, *passing through* a smart card communication device and *communication network*, and further to a *remote* central computer system.

The Office Action appears also to attribute certain central computer system functions to the access point in Hohle (Office Action, p. 3, ll. 9-11). But the access point in Hohle is described as a card reader for interfacing with a smart card, and thus is different than the remote central computer system of the claims. There is no suggestion in Hohle that the external device for signing is the issuer 10 or other remotely located central computer system.

### 4. Naccache fails to provide Motivation to Combine

The Office Action appears to further indicate that Naccache provides motivation to combine because "communication of data takes negligible time when compared to the effort for computing modular inverses" (Office Action, p. 4, ll. 12-14). Applicants respectfully submit that the motivation cited by the Office is in error, as the "negligible time" for the communication of data in Naccache is attributed to the "physical communication" through a "communication interface" or "I/O interface." The additional delay associated with communication over a communication network to a remote central computer system (e.g., as set forth in claim 1) would appear to be inconsistent the motivation asserted by the Office.

For at least the foregoing reasons, the cited references, alone or in combination, fail to constitute relevant teachings of prior arts in support of factual findings of an obviousness rejection. Applicants respectfully submit that the specified limitations in the independent claims 1, 17, 18, 21, 22, 25, and 29 are allowable. Claims 2, 4-16, 20, 23, 24, 26, 27, 30-35, and 59 each depend from these independent claims, and are believed allowable for at least the same reasons. Applicants, therefore, respectfully request that the rejections under 35 U.S.C. 103(a) be withdrawn.

## CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,

Michael L. Drapkin
Registration No. 55,127

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300

MLD/sk
61202140 v1